

CLAIMS

- Sub
a1
1. A method for generating a digital signature in a signature device for the signing of documents, comprising the steps of:
 - a) receiving input information;
 - b) creating a signature data set comprising at least the received information and a document extract value of the document for signing; and
 - c) creating an expanded digital signature by encrypting the signature data set with the aid of a signature key.
 2. The method in accordance with Claim 1, wherein said receiving input information comprises procuring the value of a signature counter.
 3. The method in accordance with Claim 2, further comprising, prior to said procuring, creating the signature counter as an attribute of the signature key.

4. The method in accordance with Claim 1 wherein the receiving input information comprises procuring an identifying characteristic to identify the signature device.
5. The method in accordance with Claim 4, wherein the receiving input information comprises procuring information as to the hardware and software environment used in creating the digital signature.
6. The method in accordance with Claim 1, further comprising entering an identifying characteristic to identify the holder of the signature key prior to said receiving input information.
7. The method in accordance with Claim 6, further comprising creating the identifying characteristic to identify the holder of the signature key as an attribute of the signature key.
8. The method in accordance with Claim 7, further comprising changing the identifying characteristic to identify the holder of the signature key prior to said receiving.

9. An electronic signature device comprising:

- a) a receiver for receiving input information;
- b) a data processor component for creating a signature data set comprising at least the received information and a document extract value of the document for signing; and
- c) an encryption component for creating an expanded digital signature by encrypting the signature data set with the aid of a signature key.

10. The signature device in accordance with Claim 9, wherein the device is a chipcard.

11. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for generating a digital signature in a signature device, said method steps comprising:

- a) receiving input information;

b) creating a signature data set comprising at least the received information and a document extract value of the document for signing;

c) creating an expanded digital signature by encrypting the signature data set with the aid of a signature key.

12. An improved digital signature, wherein the improvement comprises the inclusion of additional information in addition to a document extract value of a document for signing.

13. The improvement in accordance with Claim 12, wherein the additional information comprises information which uniquely identifies it in relation to every other digital signature generated with the same signature key.

14. The improvement in accordance with Claim 12, wherein the additional information comprises information as to the signature device with which the digital signature was executed.

15. The improvement in accordance with Claim 12 wherein the additional information comprises information on the hardware and software environment used in generating the signature.

15. The improvement in accordance with Claim 12 wherein the additional information comprises information on the hardware and software environment used in generating the signature.